entropy

MDPI

Article

Rateless Codes-Based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments

Phu Tran Tin [1,2], Tan N. Nguyen [1], Nguyen Q. Sang [3], Tran Trung Duy [4], Phuong T. Tran [5,*] and Miroslav Voznak [1]

1 VSB—Technical University of Ostrava, 17. listopadu 15/2172, 708 33 Ostrava, Czech Republic
2 Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City 700000, Vietnam
3 Department of Electrical and Electronic Engineering, Duy Tan University, DaNang City 550000, Vietnam
4 Department of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City 700000, Vietnam
5 Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
* Correspondence: tranthanhphuong@tdtu.edu.vn

Received: 30 May 2019; Accepted: 11 July 2019; Published: 16 July 2019

Abstract: In this paper, we propose a rateless codes-based communication protocol to provide security for wireless systems. In the proposed protocol, a source uses the transmit antenna selection (TAS) technique to transmit Fountain-encoded packets to a destination in presence of an eavesdropper. Moreover, a cooperative jammer node harvests energy from radio frequency (RF) signals of the source and the interference sources to generate jamming noises on the eavesdropper. The data transmission terminates as soon as the destination can receive a sufficient number of the encoded packets for decoding the original data of the source. To obtain secure communication, the destination must receive sufficient encoded packets before the eavesdropper. The combination of the TAS and harvest-to-jam techniques obtains the security and efficient energy via reducing the number of the data transmission, increasing the quality of the data channel, decreasing the quality of the eavesdropping channel, and supporting the energy for the jammer. The main contribution of this paper is to derive exact closed-form expressions of outage probability (OP), probability of successful and secure communication (SS), intercept probability (IP) and average number of time slots used by the source over Rayleigh fading channel under the joint impact of co-channel interference and hardware impairments. Then, Monte Carlo simulations are presented to verify the theoretical results.

Keywords: rateless codes; transmit antenna selection; energy harvesting; co-channel interference; hardware impairments

1. Introduction

Physical-layer security (PLS) [1–4] has attracted much attention of the researchers as an efficient method to attain security. Due to the simple implementation, i.e., only exploiting characteristics of wireless medium such as link distance and channel state information (CSI), PLS can be implemented efficiently in wireless sensor networks (WSNs), internet-of-things (IoT) networks, etc. [5–8]. To enhance the secrecy performance, diversity transmission methods can be employed. In [9–12], MIMO-based transmit–receive methods such as Transmit Antenna Selection-Maximal Ratio Combining (TAS-MRC), Maximal Ratio Transmission-MRC (MRT-MRC), MRT-Selection Combining

(MRT-SC), MRT-SC were proposed and analyzed. In addition, performance of secure communication protocols can be also enhanced with cooperative relaying methods [13–16]. In [17–20], the authors proposed cooperative jamming (CJ) techniques to reduce quality of the eavesdropping channels, where friendly jammers are employed to generate artificial noises on the eavesdropper, and the legitimate receivers have to cooperate with the jammers to remove the interference in the received signals. The results presented that the schemes which combine the diversity transmission and the jamming techniques outperform the conventional cooperative ones without using CJ. However, energy efficiency may become a critical issue when the jammer nodes continuously transmit the artificial noises by using their own energy. Recently, radio frequency (RF) energy harvesting (EH) is an efficient method to prolong lifetime for wireless networks [21–24]. Particularly, the wireless devices can harvest energy from full-energy nodes [21,22] or from power stations deployed in networks [25,26] or even from co-channel interferences caused by outside sources [27,28]. References [20,29] proposed and analyzed performance of RF-EH-based secure communication protocols. To support energy for the jammer nodes, the authors of [20,29] proposed harvest-to-jam (HJ) methods, where the cooperative jammers harvest energy from the RF signals, and then use it to generate artificial noises.

Rateless codes or Fountain codes (FCs) [30–33] have drawn much attention due to their simple implementation. In FCs, a transmitter uses Fountain encoder to generate a limitless number of encoded packets, and then transmit them to intended receivers. If the receivers can receive a sufficient number of the encoded packets, they can recover the original message of the transmitter. Due to broadcast of the wireless channels, the encoded packets can be overheard by eavesdroppers. Therefore, the security becomes a critical issue for the FCs-based communication systems. Recently, some published works considering the secure communication protocols with FCs have been reported in [34–36]. In [34], the authors proposed a secure delivery scheme, in which the security can be achieved if the legitimate user receives enough Fountain packets before the eavesdropper. In [35], a dynamic Fountain-encoded at a transmitter was proposed to enhance the data security. The authors of [36] proposed a FC-based cooperative relay protocol. In [36], the source and the jammer cooperate to remove the interference components in the received signals at the destination. Reference [37] proposed an efficient FCs-based multicast scenario to achieve security for Internet of Things (IoT) systems.

In this paper, we propose a FCs based secure communication protocol, where a multi-antenna source selects its best antenna to transmit the encoded packets to a single-antenna destination, in presence of a single-antenna eavesdropper who attempts to overhear the source information. When the destination can receive sufficient encoded packets for decoding the original data, it would send a feedback to the source to terminate the transmission. As a result, to obtain the secure transmission, the destination must receive a sufficient number of the encoded packets before the eavesdropper. Otherwise, the original information is intercepted. The main contributions of this paper can be summarized as follows:

- To the best of our knowledge, we first propose the FCs based communication protocol using the harvest-to-jam based cooperative jamming technique to reduce the quality of the eavesdropping link. Different with [34–37], we propose a cooperative jamming technique, where a cooperative jammer node harvests energy from the RF signals of the source and the interference sources to generate noises to the eavesdropper. Different with our previous works [38,39], in the proposed protocol, there exist interference sources in the network that cause co-channel interferences on both the destination and the eavesdropper.
- Until now, almost published works related to secrecy performance evaluation have assumed that the transceiver hardware of the wireless devices is perfect. However, in practice, it is not perfect due to phase noise, I/Q imbalance (IQI), amplifier non-linearity [40–43]. In this paper, the joint impact of hardware noises and co-channel interference on the system performances is investigated.
- For performance evaluation, we derive exact closed-form expressions of outage probability (OP), probability of successful and secure communication (SS), intercept probability (IP) and average

number of the time slots used by the source over Rayleigh fading channel. The closed-form formulas are easy-to-compute, and hence they can be easily used to design and optimize the considered system. In addition, all of the derived expressions are verified by Monte Carlo simulations.

The rest of this paper is organized as follows. The system model of the proposed protocols is described in Section 2. In Section 3, we evaluate performance of the proposed scheme. The simulation results are shown in Section 4. Finally, this paper is concluded in Section 5.

2. System Model

Figure 1 illustrates the system model of the proposed protocol, where the source node (S) equipped with M antennas communicates with the single-antenna destination (D), in presence of the single-antenna eavesdropper (E) who attempts to overhear the source data. All of the receivers such as D and E are suffered from co-channel interference caused by K ambient sources (denoted by $\mathrm{I}_1, \mathrm{I}_2, ..., \mathrm{I}_K$). To reduce the quality of the eavesdropping link, the cooperative jamming technique can be used, where the single antenna jammer (J) is employed to continuously generate the artificial noises to E. We assume that the nodes D and J are close with each other so that D can remove the co-channel interference generated by J [38]. Moreover, the jammer (J) uses the energy harvested from the RF signals of the source and the interference sources for transmitting the jamming signals.

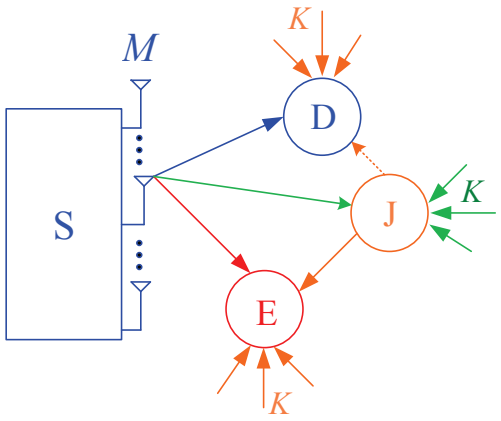

Figure 1. System model of the proposed scheme.

The source divides its original data into L packets which are encoded appropriately to create the encoded packets. Then, at each time slot, the source uses the TAS technique to send each encoded packet to the destination. At the same time, the eavesdropper tries to receive the encoded packet. The destination and the eavesdropper are assumed to be able to successfully obtain the original data if they can correctly receive at least H encoded packets, where $H = (1 + \varepsilon) L$, and ε is the decoding overhead which depends on concrete code design. Moreover, after the destination receives sufficient number of the encoded packets, it will send an ACK message to inform the source to stop the data transmission. In this case, if the eavesdropper cannot obtain enough number of the encoded packets, it cannot obtain the source data. Otherwise, the original data of the source will be intercepted.

Let us consider the data transmission at an arbitrary time slot. Let $h_{\mathrm{S}_m\mathrm{D}}$, $h_{\mathrm{S}_m\mathrm{E}}$ and $h_{\mathrm{S}_m\mathrm{J}}$ denote channel coefficients between the mth antenna of the source and the nodes D, E and J, respectively, where $m = 1, 2, ..., M$. We also denote $h_{\mathrm{I}_k\mathrm{D}}$, $h_{\mathrm{I}_k\mathrm{E}}$, $h_{\mathrm{I}_k\mathrm{J}}$ and h_{JE} as channel gains of the $\mathrm{I}_k \to \mathrm{D}$, $\mathrm{I}_k \to \mathrm{E}$, $\mathrm{I}_k \to \mathrm{J}$ and $\mathrm{J} \to \mathrm{E}$ links, respectively, where $k = 1, 2, ..., K$. We assume that all of the link channels are block and flat Rayleigh fading which keeps constant in a time slot but independently changes over

time slots. Therefore, the channel gains $\gamma_{XY} = |h_{XY}|^2, (X, Y \in \{S_m, D, E, J, I_k\})$ are exponential random variables (RVs) whose cumulative distribution function (CDF) and probability density function (PDF) are given, respectively as

$$\begin{aligned} F_{\gamma_{XY}}(z) &= 1 - \exp(-\lambda_{XY} x), \\ f_{\gamma_{XY}}(z) &= \lambda_{XY} \exp(-\lambda_{XY} x), \end{aligned} \tag{1}$$

where λ_{XY} is a parameter of γ_{XY}, i.e., $\lambda_{XY} = 1/\mathcal{E}\{\gamma_{XY}\}$, and $\mathcal{E}\{.\}$ is an expected operator. We can assume that the RVs γ_{S_mD} $(\gamma_{S_mE}, \gamma_{S_mJ})$ are independent and identical, i.e., $\lambda_{S_mD} = \lambda_{SD}$ $(\lambda_{S_mE} = \lambda_{SE}, \lambda_{S_mJ} = \lambda_{SJ})$ for all m. On the contrary, the RVs γ_{I_kD} $(\gamma_{I_kE}, \gamma_{I_kJ})$ are assumed to be independent and non-identical, i.e., $\lambda_{I_kD} \neq \lambda_{I_lD}$ $(\lambda_{I_kE} \neq \lambda_{I_lE}, \lambda_{I_kJ} \neq \lambda_{I_lJ})$ as $k \neq l$, where $l \in \{1, 2, ..., K\}$.

With the TAS technique, the source selects the best transmit antenna to send the encoded packet to the destination, using the following method:

$$b = \underset{m=1,2,...,M}{\arg\max} (\gamma_{S_mD}), \tag{2}$$

where $b \in \{1, 2, ..., M\}$.

Moreover, the CDF of γ_{S_bD} can be obtained as

$$\begin{aligned} F_{\gamma_{S_bD}}(x) &= \Pr\left(\max_{m=1,2,...,M} (\gamma_{S_mD}) < x\right) \\ &= [1 - \exp(-\lambda_{SD} x)]^M \\ &= 1 + \sum_{m=1}^{M} (-1)^m C_M^m \exp(-m\lambda_{SD} x), \end{aligned} \tag{3}$$

where $C_M^m = M!/m!/(M-m)!$ is a binomial coefficient.

Let us denote T as a block time of each time slot: a duration of αT $(0 \leq \alpha \leq 1)$ is used for the jammer node to harvest the energy from the source and the interference sources, and the remaining time $((1-\alpha)T)$ is spent for the data transmission. Then, the energy harvested by the jammer is expressed as

$$EH = \eta \alpha T \left(P_S \gamma_{S_bJ} + \sum_{k=1}^{K} P_{I_k} \gamma_{I_kJ}\right), \tag{4}$$

where η $(0 \leq \eta \leq 1)$ is an energy conversion efficiency, P_S and P_{I_k} are transmit power of the source (S) and the interference sources I_k, respectively.

Next, the average transmit power of the jammer used for the data transmission phase can be formulated by

$$P_J = \frac{EH}{(1-\alpha)T} = \chi \left(P_S \gamma_{S_bJ} + \sum_{k=1}^{K} P_{I_k} \gamma_{I_kJ}\right), \tag{5}$$

where $\chi = \eta\alpha/(1-\alpha)$.

It is worth noting that the implementation of the TAS method is simpler than that of the MRT method because it only requires the index of the best antenna which can be feed-backed by the destination (not feedback all of the channel state information (CSI) as in MRT). Moreover, the best transmit antenna selection can be performed before the EH phase, and the time used for this process can be ignored as compared with the EH and packet transmission phases. Finally, the source uses the selected antenna during each time slot for both the EH and data transmission purposes due to scheduling issues, e.g., the source uses the remaining antennas to serve other destinations.

Let us denote U as the length of each encoded packet. If the source sends the signal $x_{\mathrm{S}}[l]$ $(l = 1, 2, ..., U)$ to the destination, the received signals at the destination and the eavesdropper can be expressed, respectively as

$$\begin{aligned} y_{\mathrm{D}} &= \sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_b\mathrm{D}} \left(x_{\mathrm{S}}[l] + \nu_{\mathrm{D}}[l]\right) + \sqrt{P_{\mathrm{J}}} h_{\mathrm{JD}} x_{\mathrm{J}}[l] + \sum_{k=1}^{K} \sqrt{P_{\mathrm{I}_k}} h_{\mathrm{I}_k\mathrm{D}} x_{\mathrm{I}_k}[l] + n_{\mathrm{D}}[l], \\ y_{\mathrm{E}} &= \sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_b\mathrm{E}} \left(x_{\mathrm{S}}[l] + \nu_{\mathrm{E}}[l]\right) + \sqrt{P_{\mathrm{J}}} h_{\mathrm{JE}} x_{\mathrm{J}}[l] + \sum_{k=1}^{K} \sqrt{P_{\mathrm{I}_k}} h_{\mathrm{I}_k\mathrm{E}} x_{\mathrm{I}_k}[l] + n_{\mathrm{E}}[l], \end{aligned} \tag{6}$$

where $l = 1, 2, ..., U$, $\nu_{\mathrm{D}}[l]$ and $\nu_{\mathrm{E}}[l]$ are hardware noises caused by impairments, $x_{\mathrm{J}}[l]$ and $x_{\mathrm{I}_k}[l]$ are signals transmitted by the nodes J and I_k, respectively, and $n_{\mathrm{D}}[l]$ and $n_{\mathrm{E}}[l]$ are additive white Gaussian noises (AWGNs) at D and E, respectively. The hardware noises $\nu_{\mathrm{D}}[l]$ and $\nu_{\mathrm{E}}[l]$ can be modeled as Gaussian RVs with zero-mean and variances of κ_{D}^2 and κ_{E}^2, respectively, where κ_{D}^2 and κ_{E}^2 is total hardware impairment levels of the $\mathrm{S}_b \to \mathrm{D}$ and $\mathrm{S}_b \to \mathrm{E}$ links, respectively.

Because the nodes D and J are close with each other so that we can assume that D knows $x_{\mathrm{J}}[l]$, h_{JD} and P_{J} via securely exchanging local messages with J. Therefore, D can remove the interference component $\sqrt{P_{\mathrm{J}}} h_{\mathrm{JD}} x_{\mathrm{J}}[l]$ from the received signal y_{D}. Once D can perfectly remove the interference, the instantaneous signal-to-interference-plus-noise ratio (SINR) received by the destination under joint impact of co-channel interference and hardware impairments can be formulated as [44]

$$\begin{aligned} \Psi_{\mathrm{D}} &= \frac{P_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{D}}}{\kappa_{\mathrm{D}}^2 P_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{D}} + \sum\limits_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k\mathrm{D}} + N_0} \\ &= \frac{Q_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{D}}}{\kappa_{\mathrm{D}}^2 Q_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{D}} + \sum\limits_{k=1}^{K} Q_{\mathrm{I}_k} \gamma_{\mathrm{I}_k\mathrm{D}} + 1}, \end{aligned} \tag{7}$$

where N_0 is variance of additive noises $n_{\mathrm{D}}[l]$ which are assumed to be same at all of the receivers, $Q_{\mathrm{S}} = P_{\mathrm{S}}/N_0$ and $Q_{\mathrm{I}_k} = P_{\mathrm{I}_k}/N_0$.

Because the eavesdropper cannot remove the jamming signals, the instantaneous SINR obtained at this node is given as

$$\Psi_{\mathrm{E}} = \frac{P_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{E}}}{\kappa_{\mathrm{E}}^2 P_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{E}} + P_{\mathrm{J}} \gamma_{\mathrm{JE}} + \sum\limits_{k=1}^{K} P_{\mathrm{I}_k} \gamma_{\mathrm{I}_k\mathrm{D}} + N_0}. \tag{8}$$

Substituting (5) into (8), we obtain

$$\Psi_{\mathrm{E}} = \frac{Q_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{E}}}{\kappa_{\mathrm{E}}^2 Q_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{E}} + \chi \left(Q_{\mathrm{S}} \gamma_{\mathrm{S}_b\mathrm{J}} + \sum\limits_{k=1}^{K} Q_{\mathrm{I}_k} \gamma_{\mathrm{I}_k\mathrm{J}}\right) \gamma_{\mathrm{JE}} + \sum\limits_{k=1}^{K} Q_{\mathrm{I}_k} \gamma_{\mathrm{I}_k\mathrm{E}} + 1}. \tag{9}$$

Next, we can give expressions of the data rate for the data and eavesdropping links, respectively by

$$\begin{aligned} C_{\mathrm{D}} &= (1 - \alpha)\, \mathrm{T} \log_2 \left(1 + \Psi_{\mathrm{D}}\right), \\ C_{\mathrm{E}} &= (1 - \alpha)\, \mathrm{T} \log_2 \left(1 + \Psi_{\mathrm{E}}\right). \end{aligned} \tag{10}$$

Assume that each encoded packet can be decoded successfully if the achievable data rate is higher than a predetermined target rate (denoted by C_{th}). Otherwise, the encoded packet cannot be received correctly. Hence, the probability that the destination cannot receive one encoded packet correctly is formulated as

$$\Pr\left(C_{\mathrm{D}} < C_{\mathrm{th}}\right) = \Pr\left(\Psi_{\mathrm{D}} < \theta_{\mathrm{th}}\right) \stackrel{\Delta}{=} \rho_{\mathrm{D}}, \tag{11}$$

where

$$\theta_{\mathrm{th}} = 2^{\frac{C_{\mathrm{th}}}{(1-\alpha)\mathrm{T}}} - 1. \tag{12}$$

Note that the probability of the successful decoding for one encoded packet at D is $\Pr\left(C_{\mathrm{D}} \geq C_{\mathrm{th}}\right) = 1 - \rho_{\mathrm{D}}$. Similarly, the probability that one encoded packet can be received correctly and incorrectly by the eavesdropper is given, respectively as

$$\begin{aligned} \Pr\left(C_{\mathrm{E}} < C_{\mathrm{th}}\right) &= \Pr\left(\Psi_{\mathrm{E}} < \theta_{\mathrm{th}}\right) \stackrel{\Delta}{=} \rho_{\mathrm{E}}, \\ \Pr\left(C_{\mathrm{E}} \geq C_{\mathrm{th}}\right) &= \Pr\left(\Psi_{\mathrm{E}} \geq \theta_{\mathrm{th}}\right) = 1 - \rho_{\mathrm{E}}. \end{aligned} \tag{13}$$

Considering a delay-constrained system where the maximum number of time slots that can be used for transmitting the encoded packets is limited by N_{th} $(N_{\mathrm{th}} \geq H)$. This means that the destination cannot recover the original data if it cannot successfully receive H encoded packets within N_{th} time slots. Let us denote N_{S} $(H \leq N_{\mathrm{S}} \leq N_{\mathrm{th}})$ as the number of time slots used by the source (or the number of the encoded packets sent by the source), N_{D} and N_{E} as the number of the encoded packets received by the nodes D and E, respectively, after the source stops its transmission. Then, the outage probability (OP) at the destination is formulated by

$$\mathrm{OP} = \Pr\left(N_{\mathrm{D}} < H | N_{\mathrm{S}} = N_{\mathrm{th}}\right). \tag{14}$$

Next, the probability that the source-destination transmission is successful and secure (SS) is defined as

$$\mathrm{SS} = \Pr\left(N_{\mathrm{D}} = H, N_{\mathrm{E}} < H | N_{\mathrm{S}} \leq N_{\mathrm{th}}\right). \tag{15}$$

Equation (15) implies that the destination can receive sufficient number of the encoded packets $(N_{\mathrm{D}} = H)$ before the eavesdropper $(N_{\mathrm{E}} < H)$ when the number of time slots used is less than or equal to N_{th} $(N_{\mathrm{S}} \leq N_{\mathrm{th}})$.

Let us consider the intercept probability (IP) defined as the probability that the eavesdropper can obtain H encoded packets before or at same time with the destination:

$$\mathrm{IP} = \Pr\left(N_{\mathrm{E}} = H, N_{\mathrm{D}} \leq H | N_{\mathrm{S}} \leq N_{\mathrm{th}}\right). \tag{16}$$

We note from (16) that when the eavesdropper obtains H encoded packets, it does not need to receive more encoded packets, regardless of whether the source will transmit the encoded packets in the next time slots. Instead, it will start to decode the original data of the source. Finally, we study the average number of the time slots used to transmit encoded packets to the destination, which can be formulated by

$$\mathrm{TS} = \sum_{\mathrm{v}=0}^{\mathrm{H}-1} \mathrm{N_{th}} \Pr\left(\mathrm{N_D} = \mathrm{v} | \mathrm{N_S} = \mathrm{N_{th}}\right) + \sum_{\mathrm{t}=\mathrm{H}}^{\mathrm{N_{th}}} \mathrm{t} \Pr\left(\mathrm{N_D} = \mathrm{H} | \mathrm{N_S} = \mathrm{t}\right). \tag{17}$$

In (17), $\Pr\left(N_{\mathrm{D}} = v | N_{\mathrm{S}} = N_{\mathrm{th}}\right)$ is the probability that the number of the encoded packets received at the destination is v $(0 \leq v < H)$ when the source used N_{th} time slots (the destination is in outage), and $\Pr\left(N_{\mathrm{D}} = H | N_{\mathrm{S}} = t\right)$ is the probability that D can obtain sufficient number of the encoded packets within t time slots, where $H \leq t \leq N_{\mathrm{th}}$ (the data transmission is successful).

3. Performance Analysis

3.1. Derivations of ρ_D and ρ_E

Proposition 1. *If* $1-\kappa_D^2\theta_{th} \leq 0$, *then* $\rho_D = 1$, *and if* $1-\kappa_D^2\theta_{th} > 0$, ρ_D *can be expressed by an exact closed-form formula as*

$$\rho_D = 1 + \sum_{m=1}^{M} (-1)^m C_M^m \exp\left(-m\lambda_{SD}\omega_0\right) \prod_{k=1}^{K} \frac{\lambda_{I_kD}}{\lambda_{I_kD} + m\lambda_{SD}\omega_k}. \tag{18}$$

Proof. See the proof and notations in Appendix A. □

Proposition 2. *If* $1-\kappa_E^2\theta_{th} \leq 0$, *then* $\rho_E = 1$, *and if* $1-\kappa_E^2\theta_{th} > 0$, *we can obtain an exact closed-form expression of* ρ_E *as*

$$\begin{aligned}\rho_E = 1 &- \left(\prod_{k=1}^{K} \frac{\lambda_{I_kE}}{\lambda_{I_kE} + \lambda_{SE}\vartheta_k}\right) \exp\left(-\lambda_{SE}\vartheta_0\right) \\ &\times \left[\frac{\lambda_{JE}\Omega_{SJ}}{\lambda_{SE}}\beta_0 \exp\left(\frac{\lambda_{JE}\Omega_{SJ}}{\lambda_{SE}}\right) E_1\left(\frac{\lambda_{JE}\Omega_{SJ}}{\lambda_{SE}}\right) + \sum_{k=1}^{K} \frac{\lambda_{JE}\Omega_{I_kJ}}{\lambda_{SE}}\beta_k \exp\left(\frac{\lambda_{JE}\Omega_{I_kJ}}{\lambda_{SE}}\right) E_1\left(\frac{\lambda_{JE}\Omega_{I_kJ}}{\lambda_{SE}}\right)\right].\end{aligned} \tag{19}$$

Proof. See the proof and notations in Appendix B. □

In case where $\alpha = 0$, Equation (19) reduces to

$$\rho_E = 1 - \left(\prod_{k=1}^{K} \frac{\lambda_{I_kE}}{\lambda_{I_kE} + \lambda_{SE}\vartheta_k}\right) \exp\left(-\lambda_{SE}\vartheta_0\right). \tag{20}$$

3.2. Analysis of Outage Probability (OP)

As defined in (14), an exact closed-form expression of OP can be provided as follows:

$$OP = \sum_{N_D=0}^{H-1} C_{N_{th}}^{N_D} (1-\rho_D)^{N_D} (\rho_D)^{N_{th}-N_D}. \tag{21}$$

It is noted from (21) that the possible values of N_D are from 0 to $H-1$, and there are $C_{N_{th}}^{N_D}$ possible cases for each value of N_D.

3.3. Analysis of Successful and Secure Communication (SS)

From (15), we can rewrite SS by

$$SS = \sum_{u=H}^{N_{th}} \Pr\left(N_D = H | N_S = u\right) \times \sum_{t=0}^{H-1} \Pr\left(N_E = t | N_S = u\right). \tag{22}$$

In (22), $\Pr\left(N_D = H|N_S = u\right)$ is the probability that the destination can correctly receive H encoded packets when the number of time slots used is u. Since the data transmission between the source and the destination ends in the $u-$th time slot, $\Pr\left(N_D = H|N_S = u\right)$ is given as

$$\Pr\left(N_D = H|N_S = u\right) = C_{u-1}^{u-H} (1-\rho_D)^H (\rho_D)^{u-H}. \tag{23}$$

Moreover, $\Pr(N_{\mathrm{E}} = t|N_{\mathrm{S}} = u)$ in (22) presents the probability that the number of encoded packets obtained at the eavesdropper is t. Similar to (21), we have

$$\Pr(N_{\mathrm{E}} = t|N_{\mathrm{S}} = u) = C_u^t(1-\rho_{\mathrm{E}})^t(\rho_{\mathrm{E}})^{u-t}. \tag{24}$$

Substituting (23) and (24) into (22), an exact closed-form expression of SS can be given as

$$\mathrm{SS} = \sum_{u=H}^{N_{\mathrm{th}}} C_{u-1}^{u-H}(1-\rho_{\mathrm{D}})^H(\rho_{\mathrm{D}})^{u-H} \times \sum_{t=0}^{H-1} C_u^t(1-\rho_{\mathrm{E}})^t(\rho_{\mathrm{E}})^{u-t}. \tag{25}$$

3.4. Analysis of Intercept Probability (IP)

The intercept probability (IP) in (16) is given by

$$\mathrm{IP} = \sum_{u=H}^{N_{\mathrm{th}}} \Pr(N_{\mathrm{E}} = H|N_{\mathrm{S}} = u) \times \left[\Pr(N_{\mathrm{D}} = H|N_{\mathrm{S}} = u) + \sum_{v=0}^{H-1} \Pr(N_{\mathrm{D}} = v|N_{\mathrm{S}} = u)\right]. \tag{26}$$

In (26), $\Pr(N_{\mathrm{E}} = H|N_{\mathrm{S}} = u)$ is the probability that the eavesdropper can receive sufficient number of the encoded packets in u time slots, which can be calculated similarly to (23) as

$$\Pr(N_{\mathrm{E}} = H|N_{\mathrm{S}} = u) = C_{u-1}^{u-H}(1-\rho_{\mathrm{E}})^H(\rho_{\mathrm{E}})^{u-H}. \tag{27}$$

Next, $\Pr(N_{\mathrm{D}} = H|N_{\mathrm{S}} = u)$ in (26) is calculated by (23), and $\Pr(N_{\mathrm{D}} = v|N_{\mathrm{S}} = u)$ in (26) can be obtained by

$$\Pr(N_{\mathrm{D}} = v|N_{\mathrm{S}} = u) = C_u^v(1-\rho_{\mathrm{D}})^v(\rho_{\mathrm{D}})^{u-v}. \tag{28}$$

Plugging (23), (26), (27) and (28) together, we obtain

$$\mathrm{IP} = \sum_{u=H}^{N_{\mathrm{th}}} C_{u-1}^{u-H}(1-\rho_{\mathrm{E}})^H(\rho_{\mathrm{E}})^{u-H} \times \left[C_{u-1}^{u-H}(1-\rho_{\mathrm{D}})^H(\rho_{\mathrm{D}})^{u-H} + \sum_{v=0}^{H-1} C_u^v(1-\rho_{\mathrm{D}})^v(\rho_{\mathrm{D}})^{u-v}\right]. \tag{29}$$

3.5. Analysis of Average Number of Time Slots (TS)

Similarly, the probability $\Pr(N_{\mathrm{D}} = v|N_{\mathrm{S}} = N_{\mathrm{th}})$ and $\Pr(N_{\mathrm{D}} = H|N_{\mathrm{S}} = t)$ in (17) can be calculated respectively as

$$\begin{aligned}\Pr(N_{\mathrm{D}} = v|N_{\mathrm{S}} = N_{\mathrm{th}}) &= C_{N_{\mathrm{th}}}^v(1-\rho_{\mathrm{D}})^v(\rho_{\mathrm{D}})^{N_{\mathrm{th}}-H},\\ \Pr(N_{\mathrm{D}} = H|N_{\mathrm{S}} = t) &= C_{t-1}^{t-H}(1-\rho_{\mathrm{D}})^H(\rho_{\mathrm{D}})^{t-H}.\end{aligned} \tag{30}$$

Substituting (30) into (17), we obtain an exact closed-form formula for the average number of time slots used by the source as

$$\mathrm{TS} = N_{\mathrm{th}} \sum_{v=0}^{H-1} C_{N_{\mathrm{th}}}^v(1-\rho_{\mathrm{D}})^v(\rho_{\mathrm{D}})^{N_{\mathrm{th}}-v} + \sum_{t=H}^{N_{\mathrm{th}}} tC_{t-1}^{t-H}(1-\rho_{\mathrm{D}})^H(\rho_{\mathrm{D}})^{t-H}. \tag{31}$$

4. Simulation Results

In this section, Monte Carlo simulations are presented to verify the theoretical results. For illustration purpose, in all of the simulations, we fix the required number of the encoded packets by 10 ($H = 10$), the energy conversion efficiency by 1 ($\eta = 1$), the total block time by 1 ($\mathrm{T} = 1$), the number of the interference sources by 3 ($K = 3$), the parameters of the interference links by $\lambda_{\mathrm{I}_1\mathrm{D}} = \lambda_{\mathrm{I}_1\mathrm{E}} = \lambda_{\mathrm{I}_1\mathrm{J}} = 3$, $\lambda_{\mathrm{I}_2\mathrm{D}} = \lambda_{\mathrm{I}_2\mathrm{E}} = \lambda_{\mathrm{I}_2\mathrm{J}} = 4$ and $\lambda_{\mathrm{I}_3\mathrm{D}} = \lambda_{\mathrm{I}_3\mathrm{E}} = \lambda_{\mathrm{I}_3\mathrm{J}} = 5$, and the parameters of

the remaining links by 1 $(\lambda_{SD} = \lambda_{SE} = \lambda_{SJ} = \lambda_{JE} = 1)$. In the figures, the simulation and theoretical results are denoted by Sim and Theo, respectively.

In Figure 2, we present the probability ρ_D and ρ_E as a function of Q_S in dB. In this figure, the number of antenna equipped by the source is set to 3 $(M = 3)$, the fraction of time allocated for the EH phase is fixed by 0.3 $(\alpha = 0.3)$, the hardware impairment levels are assigned by $\kappa_D^2 = \kappa_E^2 = 0.1$, and the target rate is set to 0.75 $(C_{th} = 0.75)$. It can be seen from Figure 2 that ρ_D and ρ_E decrease with the increasing of Q_S and the decreasing of Q_I. However, ρ_D is much smaller than ρ_E at medium and high Q_S regimes. We also obverse that the simulation and theoretical results are in good agreement, which validates our derivations.

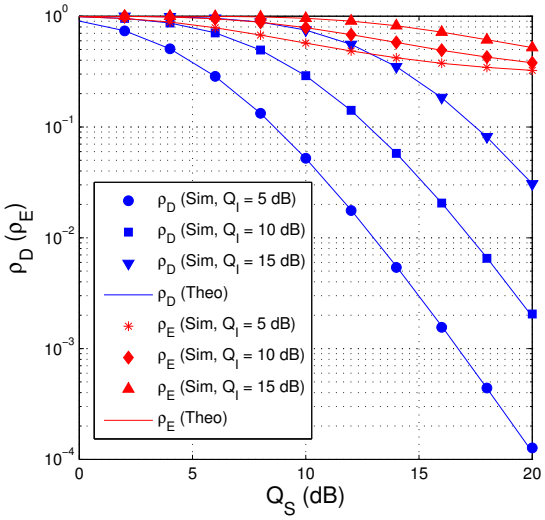

Figure 2. ρ_D and ρ_E as a function of Q_S in dB when $M = 3$, $\alpha = 0.3$, $\kappa_D^2 = \kappa_E^2 = 0.1$ and $C_{th} = 0.75$.

Figure 3 presents outage performance of the proposed protocol as a function of Q_S in dB with $Q_I = 7.5$ dB, $M = 2$, $\alpha = 0.1$, $\kappa_D^2 = \kappa_E^2 = 0$ and $C_{th} = 1$. It is shown in Figure 3 that the impact of the co-channel interference on the performance is negative, i.e., the value of OP is very high at low Q_S regimes. In particularly, when the value of Q_S is lower than that of Q_I, OP is almost equal to 1. We can also observe that the outage performance is better with high value of N_{th} because the source has more time slots to transmit the encoded packets to the destination.

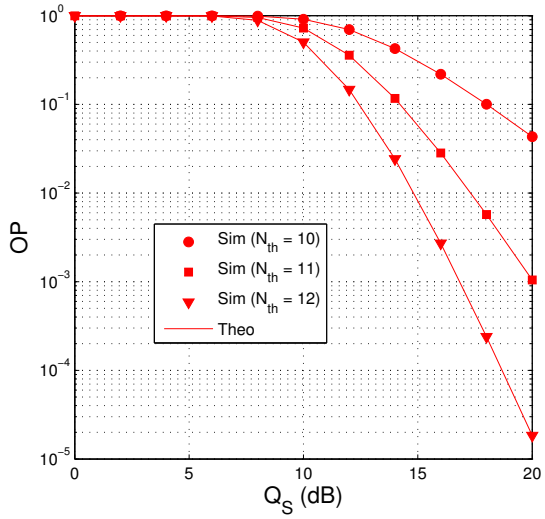

Figure 3. OP as a function of Q_S in dB when $Q_I = 7.5$ dB, $M = 2$, $\alpha = 0.1$, $\kappa_D^2 = \kappa_E^2 = 0$ and $C_{th} = 1$.

In Figure 4, we present the value of SS as a function of Q_S in dB when $Q_I = 10$ dB , $\alpha = 0.1$, $\kappa_D^2 = 0.1$, $\kappa_E^2 = 0$, $N_{th} = 20$ and $C_{th} = 1.5$. We can see that the proposed protocol obtains higher value of SS when more antennas are equipped at the source. It is also seen that when $M = 1$, the SS performance is significantly degraded because no transmit diversity gain is obtained. Moreover, SS also increases as increasing Q_S. It is due to the fact that at high Q_S values, the destination almost obtains sufficient number of the encoded packets before the eavesdropper. However, it can be seen from Figure 4 that when the value of Q_S is very high, the value of SS slightly decreases due to high overhearing possibility of the eavesdropper. Moreover, the SS performance in all values of $M(M > 1)$ is almost same at high Q_S regimes.

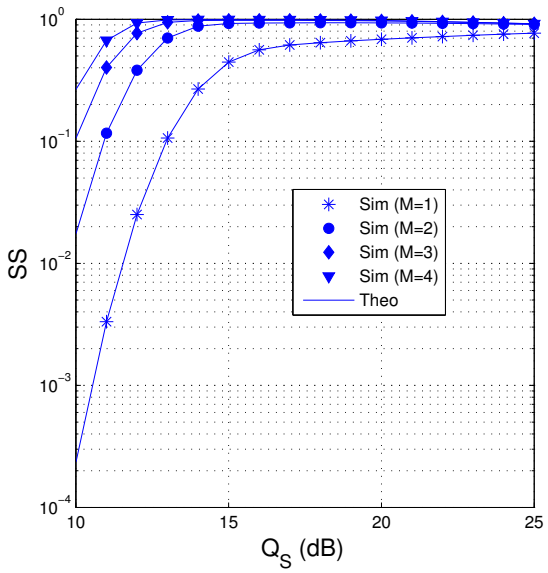

Figure 4. SS as a function of Q_S in dB when $Q_I = 10$ dB, $\alpha = 0.1$, $\kappa_D^2 = 0.1$, $\kappa_D^2 = 0$, $N_{th} = 20$ and $C_{th} = 1.5$.

In Figure 5, the value of SS is presented as a function of α when $Q_S = Q_I = 15$ dB, $M = 3$, $\kappa_E^2 = 0.1$, $N_{th} = 15$ and $C_{th} = 0.7$. As we can see, the performance significantly degrades with high hardware impairment levels of the data links, i.e., κ_D^2 is high. Moreover, we can observe from that the fraction of time allocated for the EH phase impacts on the value of SS. It can be seen that there exists an optimal value of α at which the value of SS is highest.

In Figure 6, the intercept probability of the proposed protocol is presented as a function of M when $Q_S = Q_I = 20$ dB, $\kappa_D^2 = 0.2$, $\alpha = 0.3$, $N_{th} = 20$ and $C_{th} = 0.5$. As we can see, the value of IP decreases when more antennas are equipped at the source. Also, IP is lower when the hardware impairment level of the eavesdropping links is high.

Figure 7 investigates impact of N_{th} on the intercept probability as $Q_S = Q_I = 20$ dB, $M = 2$, $\kappa_D^2 = \kappa_E^2 = 0$, and $C_{th} = 0.5$. It can be seen that the value of IP is higher when the number of N_{th} increases. However, when the number of N_{th} is high enough, IP converges to a constant. As expected, IP is lower when more time used for the EH phase (because the transmit power of the jammer is higher).

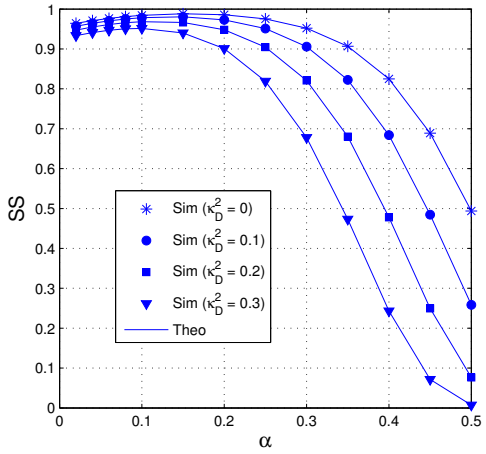

Figure 5. SS as a function of α when $Q_S = Q_I = 15$ dB, $M = 3$, $\kappa_E^2 = 0.1$, $N_{th} = 15$ and $C_{th} = 0.7$.

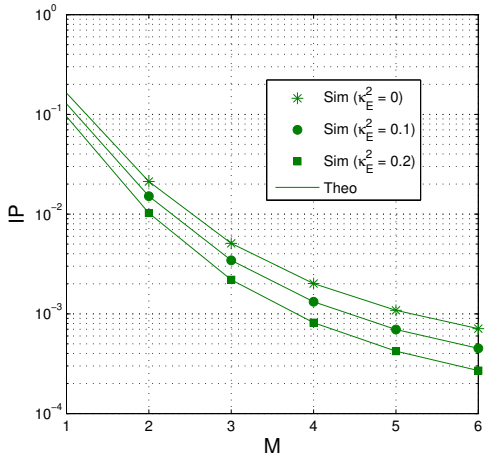

Figure 6. IP as a function of M when $Q_S = Q_I = 20$ dB, $\kappa_D^2 = 0.2$, $\alpha = 0.3$, $N_{th} = 20$ and $C_{th} = 0.5$.

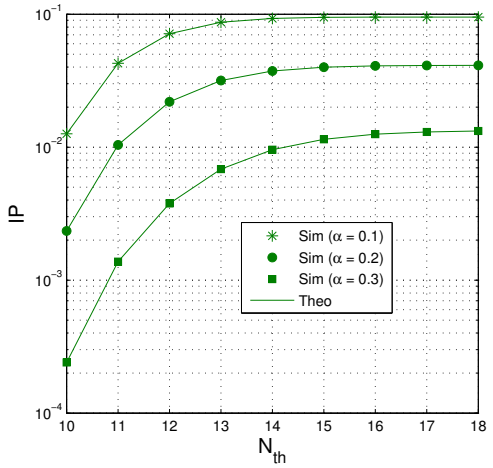

Figure 7. IP as a function of N_{th} when $Q_S = Q_I = 20$ dB, $M = 2$, $\kappa_D^2 = \kappa_E^2 = 0$ and $C_{th} = 0.5$.

Figure 8 presents OP and IP as a function of α when $Q_S = Q_I = 15$ dB, $M = 4$, $\kappa_D^2 = \kappa_E^2 = 0$ and $N_{th} = 16$. We can see that there exists a trade-off between OP and IP. Indeed, OP increases when increasing the value of α, while IP decreases with higher value of α. We can also see that when

$C_{th} = 0.8$, OP is below 10^{-3} when the value of α is higher than (about) 0.15, but the intercept probability is higher than 2.5×10^{-3}. In addition, OP significantly decreases as decreasing the value of C_{th}.

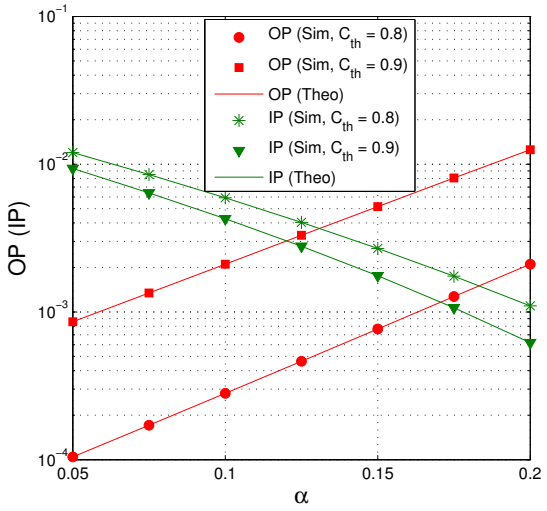

Figure 8. OP and IP as a function of α when $Q_S = Q_I = 15$ dB, $M = 4$, $\kappa_D^2 = \kappa_E^2 = 0$ and $N_{th} = 16$.

Figure 9 shows the trade-off between OP and IP when $Q_S = Q_I = 15$ dB, $M = 3$, $\kappa_D^2 = \kappa_E^2 = 0.1$ and $C_{th} = 0.75$. As we can observe, when the cooperative jamming technique is not used $(\alpha = 0)$, the OP value is lower but the IP one is higher. Similarly, to increase the reliability of the data transmission, we can increase the number of N_{th}. However, the intercept possibility of the eavesdropper also increases with higher value of N_{th}.

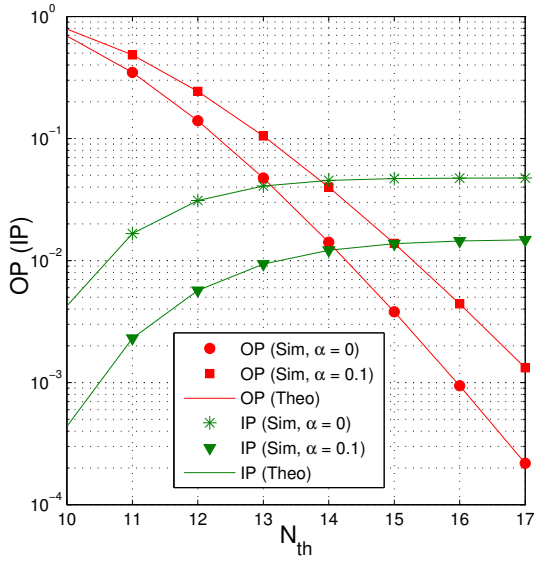

Figure 9. OP and IP as a function of N_{th} when $Q_S = Q_I = 15$ dB, $M = 3$, $\kappa_D^2 = \kappa_E^2 = 0.1$ and $C_{th} = 0.75$.

In Figure 10, we present average number of the time slots as a function of Q_S in dB when $Q_I = 10$ dB, $\alpha = 0.2$, $\kappa_D^2 = \kappa_E^2 = 0.05$, $N_{th} = 17$ and $C_{th} = 1$. We see that the number of time slots used decreases when increasing the number of antennas and the transmit power of the source. It is also seen that as the source has a single antenna ($M = 1$), the average number of time slots is much higher. Moreover, reducing the number of time slots means reducing the delay time and transmit power, which are an important metric of wireless communication systems.

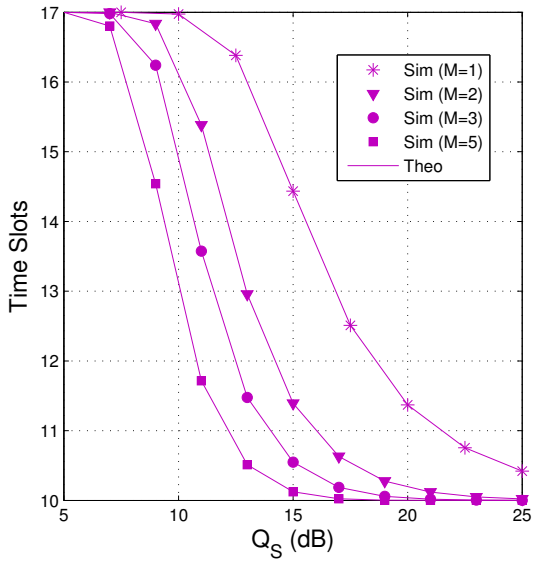

Figure 10. Average number of time slots as a function of Q_S in dB when $Q_I = 10$ dB, $\alpha = 0.2$, $\kappa_D^2 = \kappa_E^2 = 0.05$, $N_{th} = 17$ and $C_{th} = 1$.

From Figures 3–10, it is worth noting that the theoretical results and simulation results are in good agreement which validates the theoretical derivations.

5. Conclusions

In this paper, we proposed an FC-based MISO scheme using the TAS and EH-based cooperative jamming techniques for the secure communication under the joint impact of hardware impairments and co-channel interference. The performance of the proposed scheme such as outage probability (OP), probability of successful and secure communication (SS), intercept probability (IP) and average number of the time slots was evaluated via both simulation and theory. The results presented that the hardware impairment levels, the co-channel interference, the fraction of time allocated for the EH phase and the number of transmit antennas at the source significantly impact on the system performance. Moreover, there exists a trade-off between the security and reliability, i.e., between OP and IP. Finally, the fraction of time allocated for the EH phase should be designed appropriately to optimize system performance.

Author Contributions: The main contributions of P.T.T. (Phu Tran Tin) and P.T.T. (Phuong T. Tran) were to create the main ideas and execute performance evaluation by simulations, while the main contributions of T.T.D., T.N.N., M.V. and N.Q.S. are to discuss, create, and advise the main ideas and performance evaluations together.

Funding: This research received support from the grant SGS reg. No. SP2019/41 conducted at VSB Technical University of Ostrava, Czech Republic, and is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.317.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Proposition 1

From (7) and (11), we obtain

$$\begin{aligned}\rho_{\mathrm{D}} &= \Pr\left(\frac{Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}}}{\kappa_{\mathrm{D}}^2 Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}} + \sum\limits_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{D}} + 1} < \theta_{\mathrm{th}}\right) \\ &= \Pr\left(\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{D}} < \sum_{k=1}^{K} Q_{\mathrm{I}_k}\theta_{\mathrm{th}}\gamma_{\mathrm{I}_k\mathrm{D}} + \theta_{\mathrm{th}}\right). \end{aligned} \tag{A1}$$

From (A1), we observe that if $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}} \le 0$, then $\rho_{\mathrm{D}} = 1$; and if $1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}} > 0$, we can rewrite (A1) as

$$\rho_{\mathrm{D}} = \Pr\left(\gamma_{\mathrm{S}_b\mathrm{D}} < \sum_{k=1}^{K} \omega_k\gamma_{\mathrm{I}_k\mathrm{D}} + \omega_0\right), \tag{A2}$$

where

$$\omega_0 = \frac{\theta_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}}, \; \omega_k = \frac{\theta_{\mathrm{th}} Q_{\mathrm{I}_k}}{\left(1-\kappa_{\mathrm{D}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}}. \tag{A3}$$

Moreover, Equation (A2) can be rewritten by

$$\rho_{\mathrm{D}} = \int_0^{+\infty} \cdots \int_0^{+\infty} F_{\gamma_{\mathrm{S}_b\mathrm{D}}}\left(\sum_{k=1}^{K} \omega_k x_k + \omega_0\right) f_{\gamma_{\mathrm{I}_1\mathrm{D}}}(x_1) \ldots f_{\gamma_{\mathrm{I}_K\mathrm{D}}}(x_K) dx_1 \ldots dx_K. \tag{A4}$$

Using the CDF obtained by (3), we have

$$F_{\gamma_{\mathrm{S}_b\mathrm{D}}}\left(\sum_{k=1}^{K} \omega_k x_k + \omega_0\right) = 1 + \sum_{m=1}^{M} (-1)^m C_M^m \exp\left(-m\lambda_{\mathrm{SD}}\omega_0\right) \exp\left(-m\lambda_{\mathrm{SD}} \sum_{k=1}^{K} \omega_k x_k\right). \tag{A5}$$

Substituting (A5) and the PDF of $\gamma_{\mathrm{I}_k\mathrm{D}}$ in (1); after some manipulations, we can obtain (18), and finish the proof here.

Appendix B. Proof of Proposition 2

Combining (9) and (13), we have

$$\rho_{\mathrm{E}} = \Pr\left(\left(1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{E}} < \chi\theta_{\mathrm{th}}\left(Q_{\mathrm{S}}\gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{J}}\right)\gamma_{\mathrm{JE}} + \theta_{\mathrm{th}}\sum_{k=1}^{K} Q_{\mathrm{I}_k}\gamma_{\mathrm{I}_k\mathrm{E}} + \theta_{\mathrm{th}}\right). \tag{A6}$$

We observe from (A6) that if $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} \le 0$, then $\rho_{\mathrm{E}} = 1$, and if $1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}} > 0$, we can rewrite (A6) as

$$\rho_{\mathrm{E}} = \Pr\left(\gamma_{\mathrm{S}_b\mathrm{E}} < \vartheta_0 + \sum_{k=1}^{K} \vartheta_k\gamma_{\mathrm{I}_k\mathrm{E}} + \left(\mu_0\gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} \mu_k\gamma_{\mathrm{I}_k\mathrm{J}}\right)\gamma_{\mathrm{JE}}\right), \tag{A7}$$

where

$$\vartheta_0 = \frac{\theta_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}}, \; \vartheta_k = \frac{\theta_{\mathrm{th}} Q_{\mathrm{I}_k}}{\left(1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}}, \mu_0 = \frac{\chi\theta_{\mathrm{th}}}{1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}}, \; \mu_k = \frac{\chi\theta_{\mathrm{th}} Q_{\mathrm{I}_k}}{\left(1-\kappa_{\mathrm{E}}^2\theta_{\mathrm{th}}\right) Q_{\mathrm{S}}}. \tag{A8}$$

Setting $Z = \left(\mu_0 \gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} \mu_k \gamma_{\mathrm{I}_k\mathrm{J}}\right) \gamma_{\mathrm{JE}}$, from (A7), we have

$$\rho_{\mathrm{E}} = \int_0^{+\infty} \ldots \int_0^{+\infty} \left[F_{\gamma_{\mathrm{S}_b\mathrm{E}}} \left(\vartheta_0 + \sum_{k=1}^{K} \vartheta_k x_k + z \right) f_{\gamma_{\mathrm{I}_1\mathrm{E}}}(x_1) \ldots f_{\gamma_{\mathrm{I}_K\mathrm{E}}}(x_K) f_Z(z) \right] dx_1 \ldots dx_K dz. \quad \text{(A9)}$$

Substituting the CDF of $\gamma_{\mathrm{S}_b\mathrm{E}}$ and the PDF of $\gamma_{\mathrm{I}_k\mathrm{D}}$ provided by (1) into (A9), after some manipulations, which yields

$$\rho_{\mathrm{E}} = 1 - \left(\prod_{k=1}^{K} \frac{\lambda_{\mathrm{I}_k\mathrm{E}}}{\lambda_{\mathrm{I}_k\mathrm{E}} + \lambda_{\mathrm{SE}} \vartheta_k} \right) \exp\left(-\lambda_{\mathrm{SE}} \vartheta_0\right) \times \underbrace{\int_0^{+\infty} \exp\left(-\lambda_{\mathrm{SE}} z\right) f_Z(z)\, dz}_{\mathcal{I}}. \quad \text{(A10)}$$

Now, our objective is to calculate the integral $\mathcal{I}$ in (A10). At first, we rewrite $\mathcal{I}$ under the following form:

$$\begin{aligned} \mathcal{I} &= \int_0^{+\infty} \exp\left(-\lambda_{\mathrm{SE}} z\right) f_Z(z)\, dz \\ &= \int_0^{+\infty} \lambda_{\mathrm{SE}} \exp\left(-\lambda_{\mathrm{SE}} z\right) F_Z(z)\, dz. \end{aligned} \quad \text{(A11)}$$

Next, we attempt to find the CDF of Z. Setting $Y = \mu_0 \gamma_{\mathrm{S}_b\mathrm{J}} + \sum_{k=1}^{K} \mu_k \gamma_{\mathrm{I}_k\mathrm{J}}$, the CDF of Z can be formulated by

$$\begin{aligned} F_Z(z) &= \Pr\left(Y \gamma_{\mathrm{JE}} < z\right) \\ &= \int_0^{+\infty} F_Y\left(\frac{z}{x}\right) \lambda_{\mathrm{JE}} \exp\left(-\lambda_{\mathrm{JE}} x\right) dx. \end{aligned} \quad \text{(A12)}$$

Before calculating the CDF of Y, we note that Y is sum of the exponential RVs, i.e., $\mu_0 \gamma_{\mathrm{S}_b\mathrm{J}}$ and $\mu_k \gamma_{\mathrm{I}_k\mathrm{J}}$. Indeed, because $\gamma_{\mathrm{S}_b\mathrm{J}}$ and $\gamma_{\mathrm{I}_k\mathrm{J}}$ are exponential RVs whose parameters are λ_{SJ} and $\lambda_{\mathrm{I}_k\mathrm{J}}$, respectively, hence $\mu_0 \gamma_{\mathrm{S}_b\mathrm{J}}$ and $\mu_k \gamma_{\mathrm{I}_k\mathrm{J}}$ are also exponential RVs, and their parameters are $\lambda_{\mathrm{SJ}}/\mu_0$ and $\lambda_{\mathrm{I}_k\mathrm{J}}/\mu_k$, respectively. Hence, the CDF of Y can be given as

$$F_Y(y) = 1 - \beta_0 \exp\left(-\Omega_{\mathrm{SJ}} y\right) - \sum_{k=1}^{K} \beta_k \exp\left(-\Omega_{\mathrm{I}_k\mathrm{J}} y\right), \quad \text{(A13)}$$

where

$$\Omega_{\mathrm{SJ}} = \frac{\lambda_{\mathrm{SJ}}}{\mu_0}, \Omega_{\mathrm{I}_k\mathrm{J}} = \frac{\lambda_{\mathrm{I}_k\mathrm{J}}}{\mu_k}, \beta_0 = \prod_{k=1}^{K} \frac{\Omega_{\mathrm{I}_k\mathrm{J}}}{\Omega_{\mathrm{I}_k\mathrm{J}} - \Omega_{\mathrm{SJ}}}, \beta_k = \frac{\Omega_{\mathrm{SJ}}}{\Omega_{\mathrm{SJ}} - \Omega_{\mathrm{I}_k\mathrm{J}}} \prod_{t=1, t\neq k}^{K} \frac{\Omega_{\mathrm{I}_t\mathrm{J}}}{\Omega_{\mathrm{I}_t\mathrm{J}} - \Omega_{\mathrm{I}_k\mathrm{J}}}. \quad \text{(A14)}$$

Substituting (A13) into (A12), we obtain

$$\begin{aligned} F_Z(z) = 1 &- \beta_0 \int_0^{+\infty} \lambda_{\mathrm{JE}} \exp\left(-\lambda_{\mathrm{JE}} x\right) \exp\left(-\Omega_{\mathrm{SJ}} \frac{z}{x}\right) dy \\ &- \sum_{k=1}^{K} \beta_k \int_0^{+\infty} \lambda_{\mathrm{JE}} \exp\left(-\lambda_{\mathrm{JE}} x\right) \exp\left(-\Omega_{\mathrm{I}_k\mathrm{J}} \frac{z}{x}\right) dy. \end{aligned} \quad \text{(A15)}$$

Using (Equation (3.324.1) of [45]) for the corresponding integrals in (A15), we arrive at

$$F_Z(z) = 1 - 2\beta_0\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}z}K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}z}\right) - \sum_{k=1}^{K} 2\beta_k\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}z}K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}z}\right), \tag{A16}$$

where $K_1(.)$ is modified Bessel function of the second kind [45]. Then, substituting (A16) into (A11), we obtain (A17) as

$$\mathcal{I} = 1 - 2\beta_0\int_0^{+\infty}\lambda_{\mathrm{SE}}\exp\left(-\lambda_{\mathrm{SE}}z\right)\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}z}K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}z}\right)dz - \sum_{k=1}^{K} 2\beta_k\int_0^{+\infty}\lambda_{\mathrm{SE}}\exp\left(-\lambda_{\mathrm{SE}}z\right)\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}z}K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}z}\right)dz. \tag{A17}$$

Next, changing variable $t = \sqrt{z}$, we can rewrite (A17) as

$$\mathcal{I} = 1 - 4\lambda_{\mathrm{SE}}\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}\beta_0\int_0^{+\infty}t^2\exp\left(-\lambda_{\mathrm{SE}}t^2\right)K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}t\right)dt - \sum_{k=1}^{K} 4\lambda_{\mathrm{SE}}\sqrt{\Omega_{\mathrm{I}_k\mathrm{J}}\lambda_{\mathrm{JE}}}\beta_k\int_0^{+\infty}t^2\exp\left(-\lambda_{\mathrm{SE}}t^2\right)K_1\left(2\sqrt{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}t\right)dt. \tag{A18}$$

Applying (Equation (6.631.3) of [45]) for the corresponding integrals in (A18), we obtain

$$\mathcal{I} = 1 - \beta_0\exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{2\lambda_{\mathrm{SE}}}\right)W_{-1,1/2}\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right) - \sum_{k=1}^{K}\beta_k\exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{2\lambda_{\mathrm{SE}}}\right)W_{-1,1/2}\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right), \tag{A19}$$

where $W_{-1,1/2}(.)$ is the Whittaker function [45].

Moreover, from (Equation (46) of [46]), we have

$$\exp\left(\frac{x}{2}\right)W_{-1,1/2}(x) = 1 - x\exp(x)E_1(x), \tag{A20}$$

where $E_1(.)$ is exponential integral function [45].

Combining (A19) and (A20), after some manipulations, we obtain

$$\mathcal{I} = \frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\beta_0\exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right)E_1\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{SJ}}}{\lambda_{\mathrm{SE}}}\right) + \sum_{k=1}^{K}\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\beta_k\exp\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right)E_1\left(\frac{\lambda_{\mathrm{JE}}\Omega_{\mathrm{I}_k\mathrm{J}}}{\lambda_{\mathrm{SE}}}\right). \tag{A21}$$

It is worth noting that to attain (A21), we used the following equation:

$$\beta_0 + \sum_{k=1}^{K}\beta_k = 1. \tag{A22}$$

Finally, substituting (A21) into (A10), we obtain (19), and finish the proof.

References

1. Wyner, A.D. The Wire-tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Csiszar, I.; Korner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *2*, 339–348. [CrossRef]

3. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R.D. Discrete Memoryless Interference and Broadcast Channels with Conffdential Messages: Secrecy Rate Regions. *IEEE Trans. Inf. Theory* **2008**, *2*, 2493–2507. [CrossRef]
4. Gopala, P.K.; Lai, L.; Gamal, H.E. On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *2*, 4687–4698. [CrossRef]
5. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy* **2017**, *19*, 420. [CrossRef]
6. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *2*, 730. [CrossRef]
7. Tin, P.T.; Hung, D.T.; Tan, N.N.; Duy, T.T.; Voznak, M. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission With and Without Presence of Hardware Impairments. *Entropy* **2019**, *21*, 217. [CrossRef]
8. Tin, P.T.; Nam, P.M.; Duy, T.T.; Phuong, T.T.; Voznak, M. Secrecy Performance of TAS/SC-based Multi-hop Harvest-to-Transmit Cognitive WSNs under Joint Constraint of Interference and Hardware Imperfection. *Sensors* **2019**, *19*, 1160. [CrossRef] [PubMed]
9. Zhang, T.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W. Secure Transmission in Cognitive MIMO Relaying Networks With Outdated Channel State Information. *IEEE Access* **2016**, *4*, 8212–8224. [CrossRef]
10. Huang, Y.; Wang, J.; Zhong, C.; Duong, T.Q.; Karagiannidis, G.K. Secure Transmission in Cooperative Relaying Networks with Multiple Antennas. *IEEE Trans. Wirel. Commun.* **2016**, *2*, 6843–6856. [CrossRef]
11. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Secure Multiuser Scheduling in Downlink Dual-hop Regenerative Relay Networks over Nakagami-m Fading Channels. *IEEE Trans. Wirel. Commun.* **2016**, *2*, 8009–8024. [CrossRef]
12. Zhao, R.; Lin, H.; He, Y.-C.; Chen, D.-H.; Huang, Y.; Yang, L. Secrecy Performance of Transmit Antenna Selection for MIMO Relay Systems with Outdated CSI. *IEEE Trans. Commun.* **2018**, *2*, 546–559. [CrossRef]
13. Mo, J.; Tao, M.; Liu, L. Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Commun. Lett.* **2012**, *2*, 878–881.
14. Lee, J.-H.; Sohn, I.; Kim, Y.-H. Transmit Power Allocation for Physical Layer Security in Cooperative Multi-Hop Full-Duplex Relay Networks. *Sensors* **2016**, *2*, 1726. [CrossRef] [PubMed]
15. Keshav, S.; Ku, M.-L.; Biswas, S.; Ratnarajah, T. Energy-Efficient Subcarrier Pairing and Power Allocation for DF Relay Networks with an Eavesdropper. *Energies* **2017**, *2*, 1953.
16. Hieu, T.D.; Duy, T.T.; Kim, B.-S. Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs with Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises. *IEEE Sens. J.* **2018**, *2*, 5173–5186. [CrossRef]
17. Cao, K.; Cai, K.; Wu, Y.; Yang, W. Cooperative Jamming for Secure Communication with Finite Alphabet Inputs. *IEEE Commun. Lett.* **2017**, *2*, 2025–2028. [CrossRef]
18. Kang, J.M.; Yang, J.; Ha, J.; Kim, I.M. Joint Design of Optimal Precoding and Cooperative Jamming for Multiuser Secure Broadcast Systems. *IEEE Trans. Veh. Technol.* **2017**, *2*, 10551–10556. [CrossRef]
19. Ma, H.; Cheng, J.; Wang, X.; Ma, P. Robust MISO Beamforming with Cooperative Jamming for Secure Transmission From Perspectives of QoS and Secrecy Rate. *IEEE Trans. Commun.* **2018**, *2*, 767–780. [CrossRef]
20. Zhang, G.; Xu, J.; Wu, Q.; Cui, M.; Li, X.; Lin, F. Wireless Powered Cooperative Jamming for Secure OFDM System. *IEEE Trans. Veh. Technol.* **2018**, *2*, 1331–1346. [CrossRef]
21. Nasir, A.A.; Zhou, X.; Durrani, S.; Kennedy, R.A. Relaying Protocols for Wireless Energy Harvesting and Information Processing. *IEEE Trans. Wirel. Commun.* **2013**, *2*, 3622–3636. [CrossRef]
22. Atapattu, S.; Evans, J. Optimal Energy Harvesting Protocols for Wireless Relay Networks. *IEEE Trans. Wirel. Commun.* **2016**, *2*, 5789–5803. [CrossRef]
23. Wang, L.; Wong, K.K.; Jin, S.; Zheng, G.; Heath, R.W. A New Look at Physical Layer Security, Caching, and Wireless Energy Harvesting for Heterogeneous Ultra-Dense Networks. *IEEE Commun. Mag.* **2018**, *2*, 49–55. [CrossRef]
24. Chang, S.; Li, J.; Fu, X.; Zhang, L. Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing. *Entropy* **2017**, *19*, 462. [CrossRef]
25. Xu, C.; Zheng, M.; Liang, W.; Yu, H.; Liang, Y.C. Outage Performance of Underlay Multihop Cognitive Relay Networks with Energy Harvesting. *IEEE Commun. Lett.* **2016**, *2*, 1148–1151. [CrossRef]

26. Xu, C.; Zheng, M.; Liang, W.; Yu, H.; Liang, Y.C. End-to-end Throughput Maximization for Underlay Multi-hop Cognitive Radio Networks with RF Energy Harvesting. *IEEE Trans. Wirel. Commun.* **2017**, *2*, 3561–3572. [CrossRef]
27. Zhu, G.; Zhong, C.; Suraweera, H.A.; Karagiannidis, G.K.; Zhang, Z.; Tsiftsis, T.A. Wireless Information and Power Transfer in Relay Systems with Multiple Antennas and Interference. *IEEE Trans. Commun.* **2015**, *2*, 1400–1418. [CrossRef]
28. Chen, E.; Xia, M.; Da Costa, D.; Aissa, S. Multi-hop Cooperative Relaying with Energy Harvesting from Co-Channel Interferences. *IEEE Commun. Lett.* **2017**, *2*, 1199–1202. [CrossRef]
29. Liu, M.; Liu, Y. Power Allocation for Secure SWIPT Systems with Wireless-Powered Cooperative Jamming. *IEEE Commun. Lett.* **2017**, *2*, 1353–1356. [CrossRef]
30. MacKay, D. Fountain Codes. *IEE Proc. Commun.* **2005**, *2*, 1331–1346. [CrossRef]
31. Castura, J.; Mao, Y. Rateless Coding over Fading Channels. *IEEE Commun. Lett.* **2006**, *2*, 46–48. [CrossRef]
32. Nguyen, H.D.T.; Tran, L.N.; Hong, E.K. On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes. *IEEE Commun. Lett.* **2011**, *2*, 569–571. [CrossRef]
33. Yue, J.; Lin, Z.; Vucetic, B. Distributed Fountain Codes With Adaptive Unequal Error Protection in Wireless Relay Networks. *IEEE Trans. Wirel. Commun.* **2014**, *2*, 4220–4231. [CrossRef]
34. Niu, H.; Iwai, M.; Sezaki, K.; Sun, L.; Du, Q. Exploiting Fountain Codes for Secure Wireless Delivery. *IEEE Commun. Lett.* **2014**, *2*, 777–780. [CrossRef]
35. Li, W.; Du, Q.; Sun, L.; Ren, P.; Wang, Y. Security Enhanced via Dynamic Fountain Code Design for Wireless Delivery. In Proceedings of the IEEE 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–6.
36. Sun, L.; Ren, P.; Du, Q.; Wang, Y. Fountain-coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2016**, *2*, 291–300. [CrossRef]
37. Du, Q.; Xu, Y.; Li, W.; Song, H. Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 8404219. [CrossRef]
38. Hung, D.T.; Duy, T.T.; Trinh, D.Q.; Bao, V.N.Q. Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments. In Proceedings of the 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Ho Chi Minh City, Vietnam, 29–31 January 2018; pp. 164–169.
39. Hung, D.T.; Duy, T.T.; Trinh, D.Q.; Bao, V.N.Q.; Hanh, T. Security-Reliability Analysis of Power Beacon-Assisted Multi-hop Relaying Networks Exploiting Fountain Codes with Hardware Imperfection. In Proceedings of the International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 18–20 October 2018; pp. 354–359.
40. Mokhtar, M.; Gomaa, A.; Al-Dhahir, N. OFDM AF Relaying under I/Q Imbalance: Performance Analysis and Baseband Compensation. *IEEE Trans. Commun.* **2013**, *2*, 1304–1313. [CrossRef]
41. Björnson, E.; Matthaiou, M.; Debbah, M. A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments. *IEEE Trans. Commun.* **2013**, *2*, 4512–4525. [CrossRef]
42. Son, P.N.; Kong, H.Y. Energy-Harvesting Decode-and-Forward Relaying under Hardware Impairments. *Wirel. Pers. Commun.* **2017**, *2*, 6381–6395. [CrossRef]
43. Solanki, S.; Upadhyay, P.K.; da Costa, D.B.; Bithas, P.S.; Kanatas, A.G.; Dias, U.S. Joint Impact of RF Hardware Impairments and Channel Estimation Errors in Spectrum Sharing Multiple-Relay Networks. *IEEE Trans. Commun.* **2018**, *2*, 3809–3824. [CrossRef]
44. Zarei, S.; Gerstacker, W.H.; Aulin, J.; Schober, R. Multi-Cell Massive MIMO Systems with Hardware Impairments: Uplink-Downlink Duality and Downlink Precoding. *IEEE Trans. Wirel. Commun.* **2017**, *2*, 5115–5130. [CrossRef]
45. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier Inc.: San Diego, CA, USA, 2007.
46. Duy, T.T.; Alexandropoulos, G.C.; Vu, T.T.; Vo, N.-S.; Duong, T.Q. Outage Performance of Cognitive Cooperative Networks with Relay Selection over Double-Rayleigh Fading Channels. *IET Commun.* **2016**, *2*, 57–64. [CrossRef]